FIG. 1

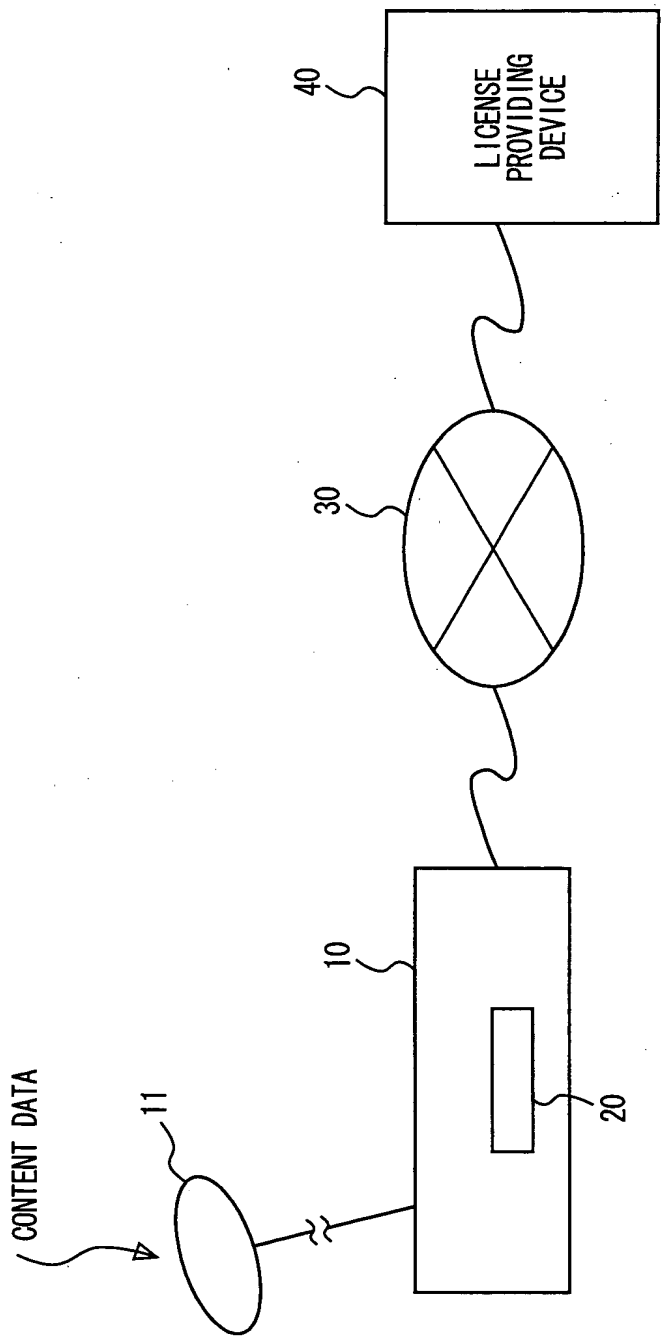


FIG. 2

SYMBOL	NAME	ATTRIBUTE	CHARACTERISTICS
Dc	DATA	PECULIAR TO DATA	EX.: MUSIC, READING, EDUCATIONAL OR IMAGE DATA, RECORDED AND MANAGED AS ENCRYPTED CONTENT DATA E(Kc, Dc) ENCRYPTED WITH Kc
Di	DATA INFORMATION	PECULIAR TO DATA	PLAINTEXT DATA RELATED TO Dc AND INCLUDING DID
DID	DATA ID	PECULIAR TO DATA	MANAGEMENT CODE FOR SPECIFYING Dc AND Kc
Kc	CONTENT KEY	PECULIAR TO DATA	SYMMETRIC KEY ENCRYPTING/DECRYPTING ENCRYPTED DATA
AC	CONTROL INFORMATION	PECULIAR TO LICENSE	RESTRICTIONS RELATED TO REPRODUCTION AND LICENSE HANDLING
LID	LICENSE ID	PECULIAR TO LICENSE	MANAGEMENT CODE FOR SPECIFYING LICENSE
LIC	LICENSE	PECULIAR TO LICENSE	GENERALLY REPRESENTING Kc//AC//DID//LID

FIG. 3

	SYMBOL	NAME	CHARACTERISTIC
LICENSE PROVIDING DEVICE	KPa	CERTIFICATION KEY	PUBLIC DECRYPTION KEY FOR VERIFYING CERTIFICATE BY CERTIFICATION AUTHORITY OPERATED BY LICENSE PROVIDER SIDE
	Ks1x	SESSION KEY	TEMPORARY KEY PRODUCED FOR EVERY LICENSE DISTRIBUTION SYMMETRIC KEY
DATA STORAGE DEVICE (HARD DISK)	Ka	MASTER KEY	PRIVATE ENCRYPTION KEY TO BE USED FOR PRODUCING CLASS CERTIFICATE OPERATED BY CERTIFICATION AUTHORITY
	KPa	CERTIFICATION KEY	PUBLIC DECRYPTION KEY FOR VERIFYING CERTIFICATE BY CERTIFICATION AUTHORITY OPERATED BY LICENSE PROVIDER SIDE
	KPcmy	CLASS PUBLIC KEY	ENCRYPTION KEY ASSIGNED TO CLASS (UNIT SUCH AS TYPE) OF DEVICE "y" IS IDENTIFIER IDENTIFYING CLASS
	Kcmy	CLASS PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH CLASS PUBLIC KEY KPcmy
	Icmy	CLASS INFORMATION	INFORMATION DATA OF DEVICE AND CLASS PUBLIC KEY IN EACH CLASS
	Cmy	CLASS CERTIFICATE	Cmy=KPcmy//Icmy//E(Ka, H(KPcmy//Icmy)) CORRECTNESS IS VERIFIED WITH CERTIFICATION KEY KPa
	KPomz	INDIVIDUAL PUBLIC KEY	INDIVIDUAL PUBLIC ENCRYPTION KEY HAVING VALUE PECULIAR TO EACH DATA STORAGE DEVICE "z" IS IDENTIFIER IDENTIFYING DATA STORAGE DEVICE
	Komz	INDIVIDUAL PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH INDIVIDUAL PUBLIC KEY KPomz
	Ks1x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE PROVIDER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY
	Ks2x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE RECEIVER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY
REPRODUCING CIRCUIT	KPcpy	CLASS PUBLIC KEY	ENCRYPTION KEY ASSIGNED TO CLASS (UNIT SUCH AS TYPE) OF DEVICE "y" IS IDENTIFIER IDENTIFYING CLASS
	Kcpy	CLASS PRIVATE KEY	ASYMMETRIC DECRYPTION KEY DECRYPTING DATA ENCRYPTED WITH CLASS PUBLIC KEY KPcpy
	Icpy	CLASS INFORMATION	INFORMATION DATA OF DEVICE AND CLASS PUBLIC KEY IN EACH CLASS
	Cpy	CLASS CERTIFICATE	Cpy=KPcpy//Icpy//E(Ka, H(KPcpy//Icpy)) CORRECTNESS IS VERIFIED WITH CERTIFICATION KEY KPa
	Ks2x	SESSION KEY	TEMPORARY KEY PRODUCED BY LICENSE RECEIVER SIDE FOR EVERY LICENSE TRANSMISSION SYMMETRIC KEY

FIG. 4

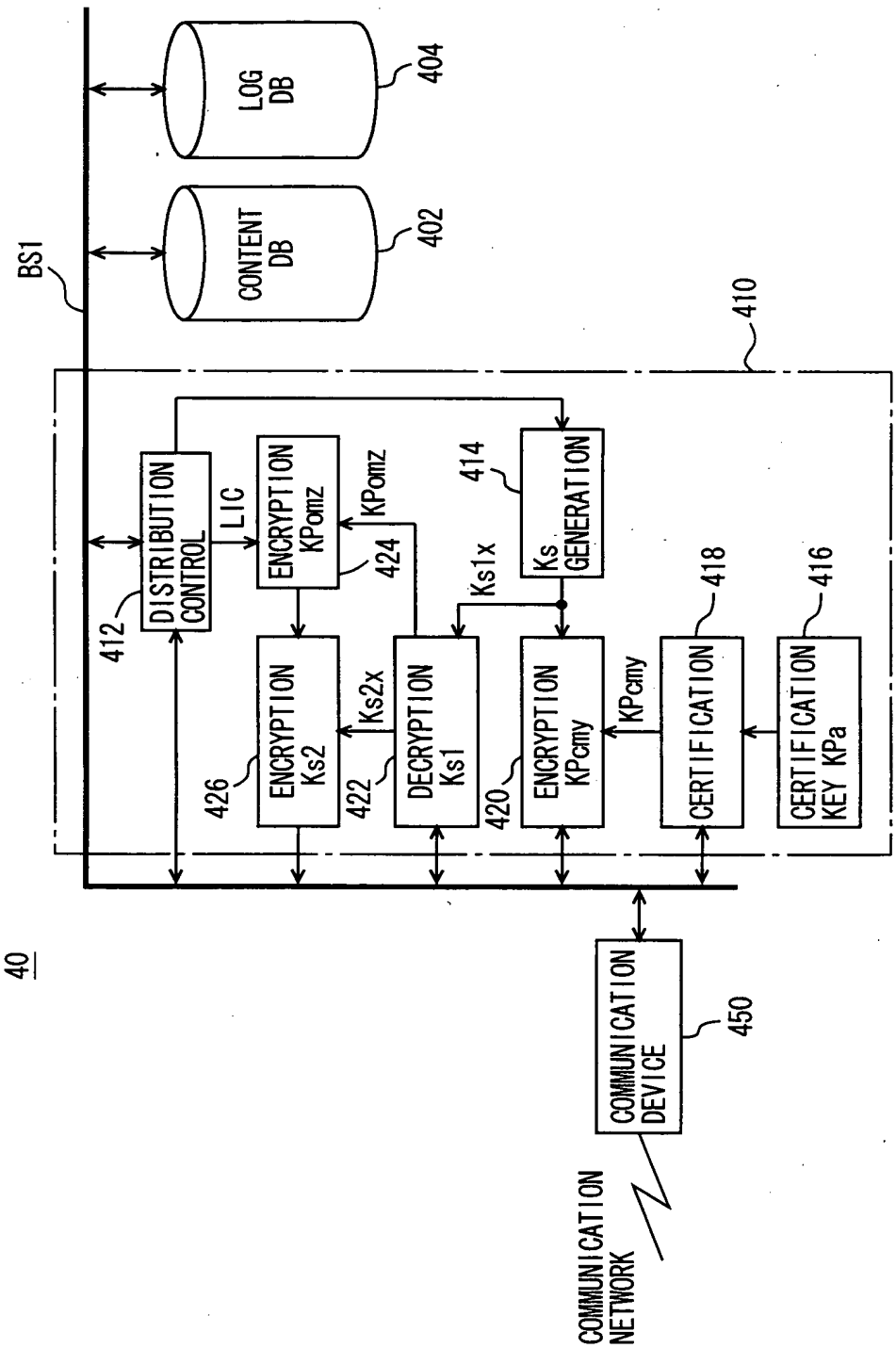


FIG. 5

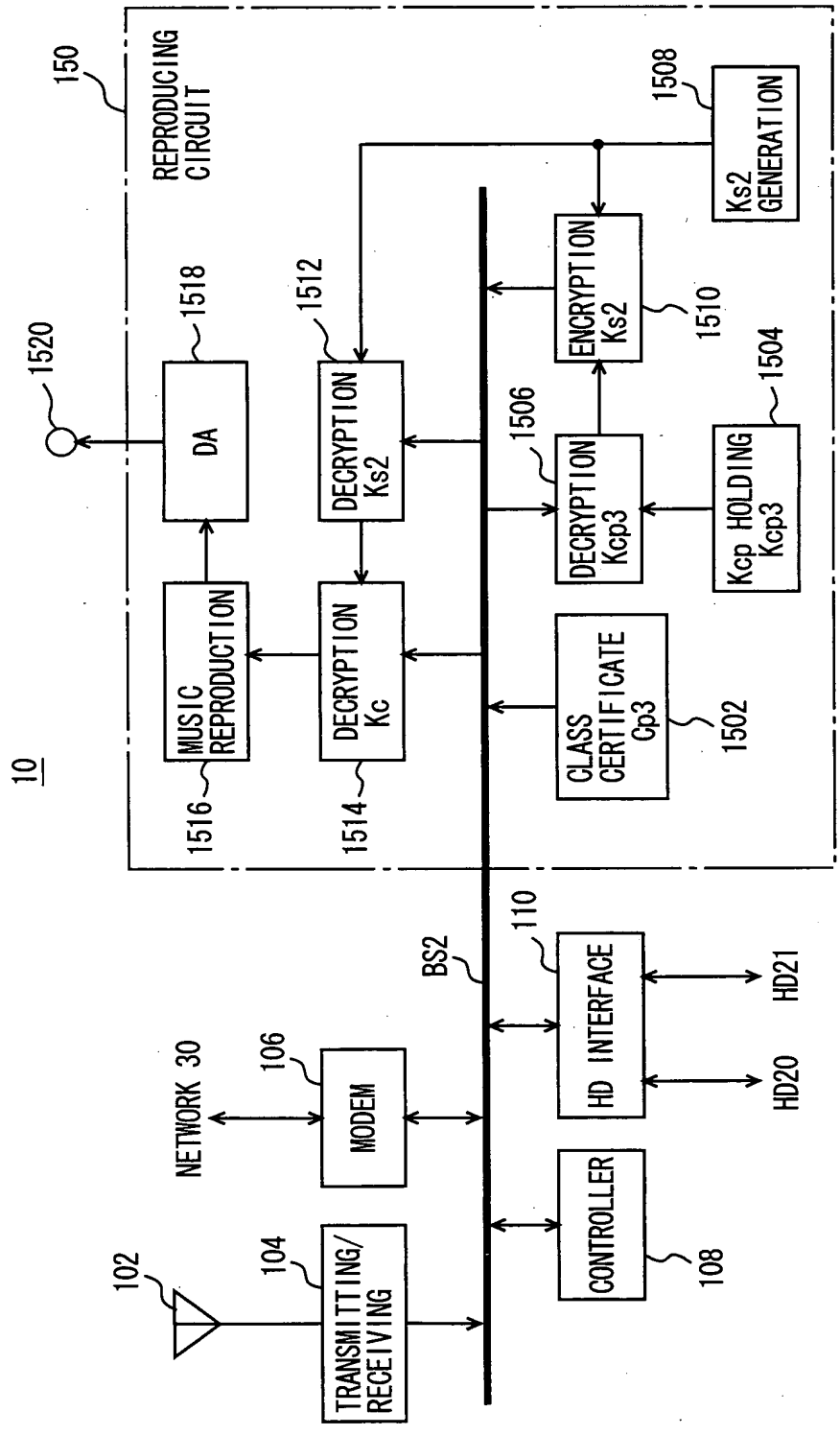


FIG. 6

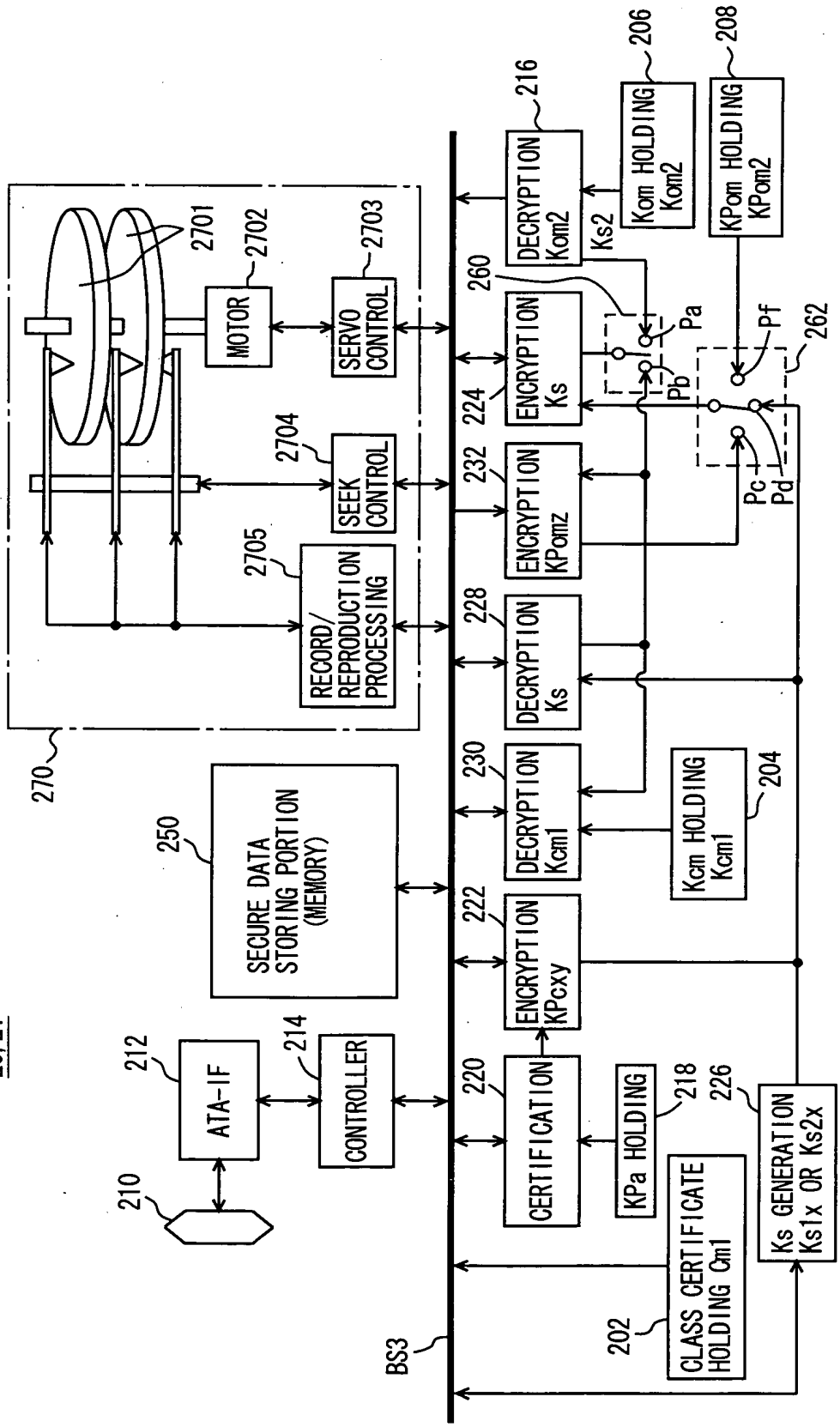


FIG. 7

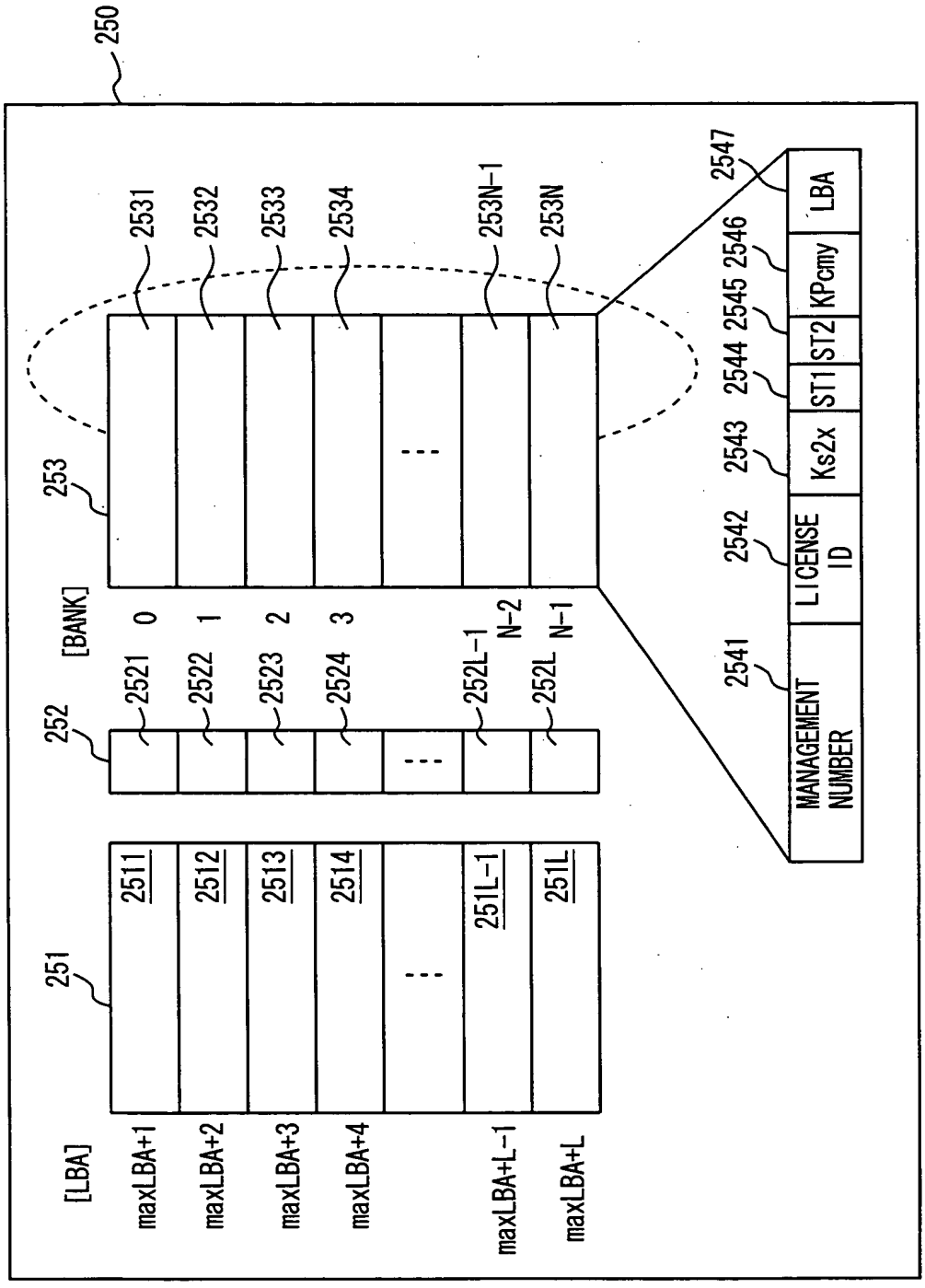


FIG. 8

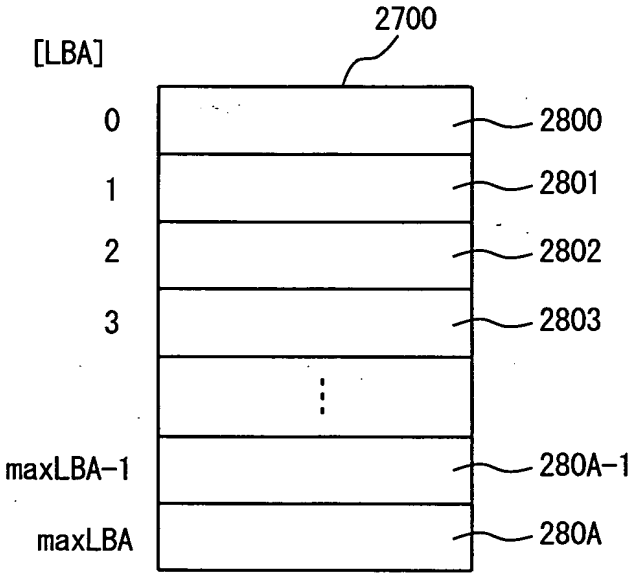


FIG. 9

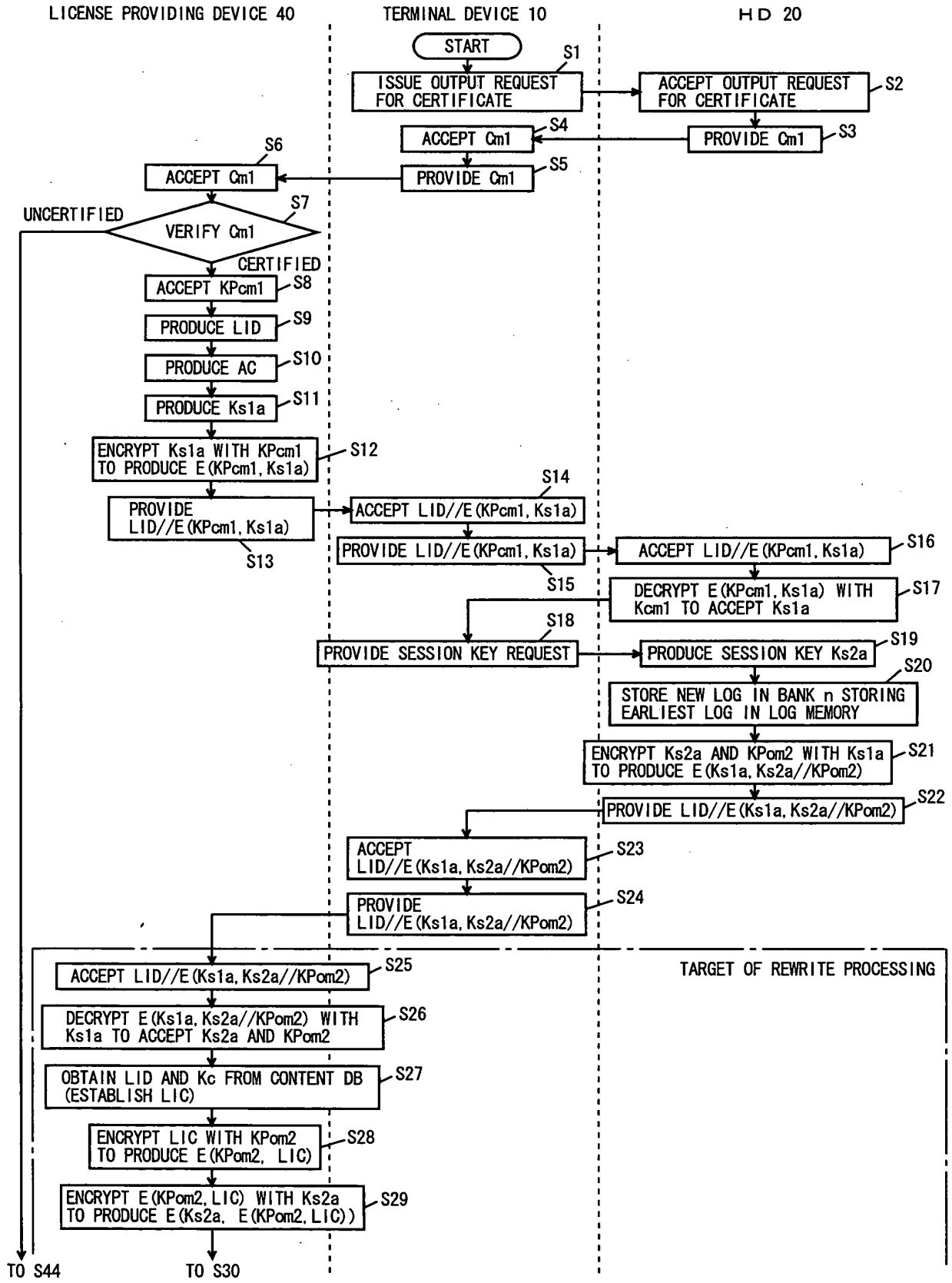


FIG. 10

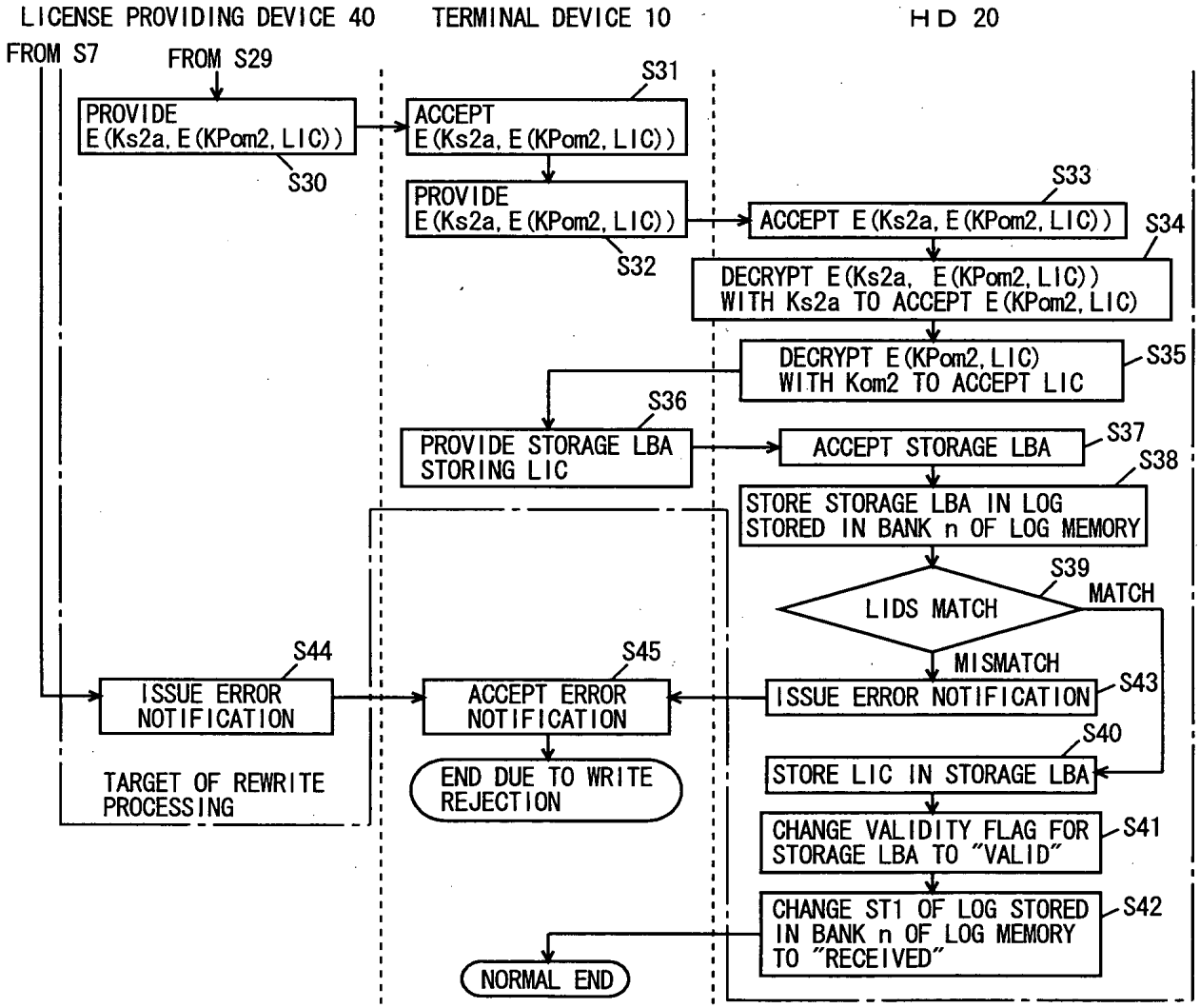


FIG. 11

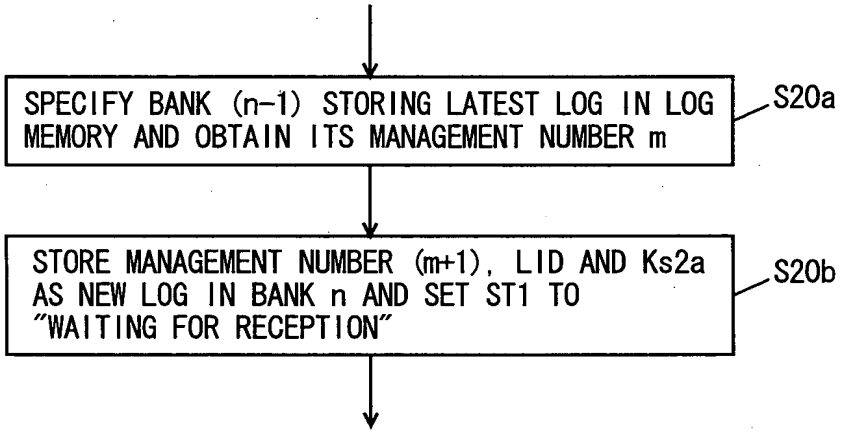


FIG. 12

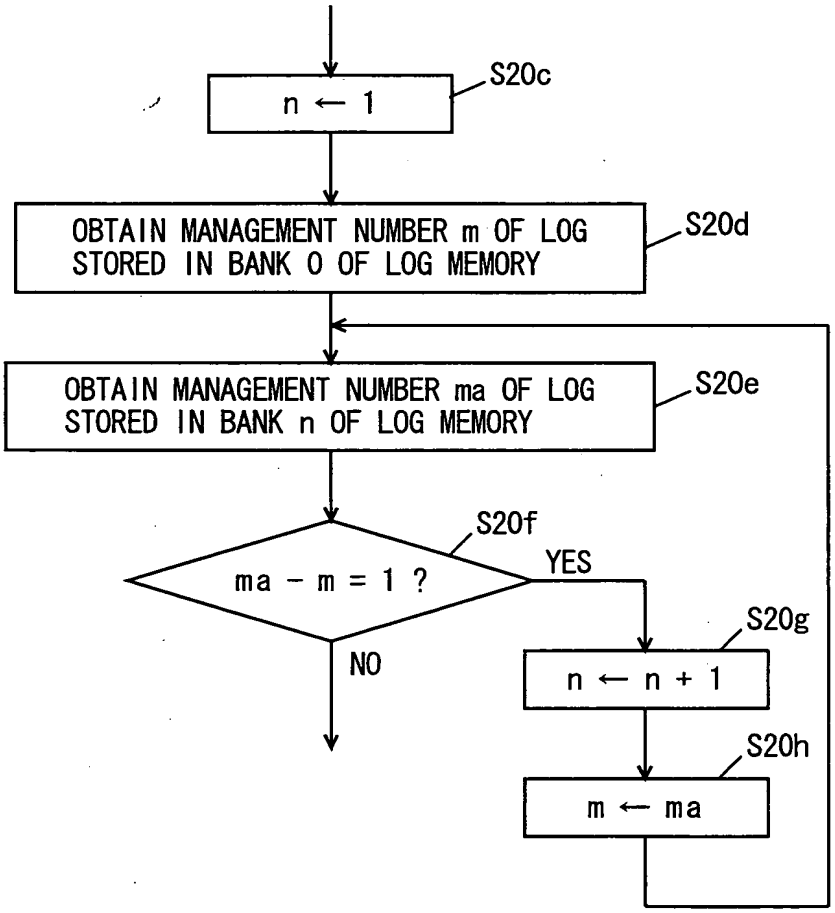


FIG. 13

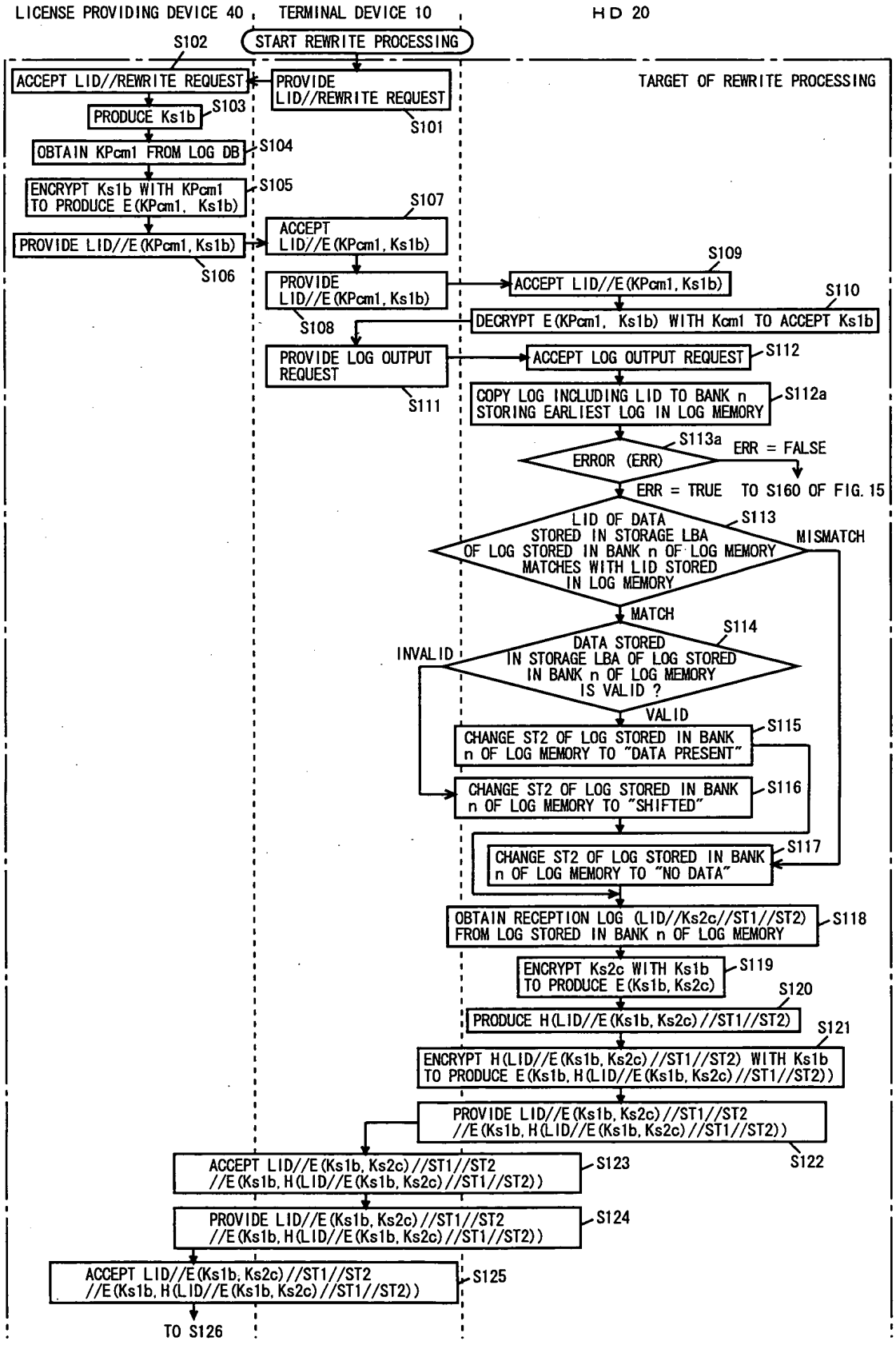


FIG. 14

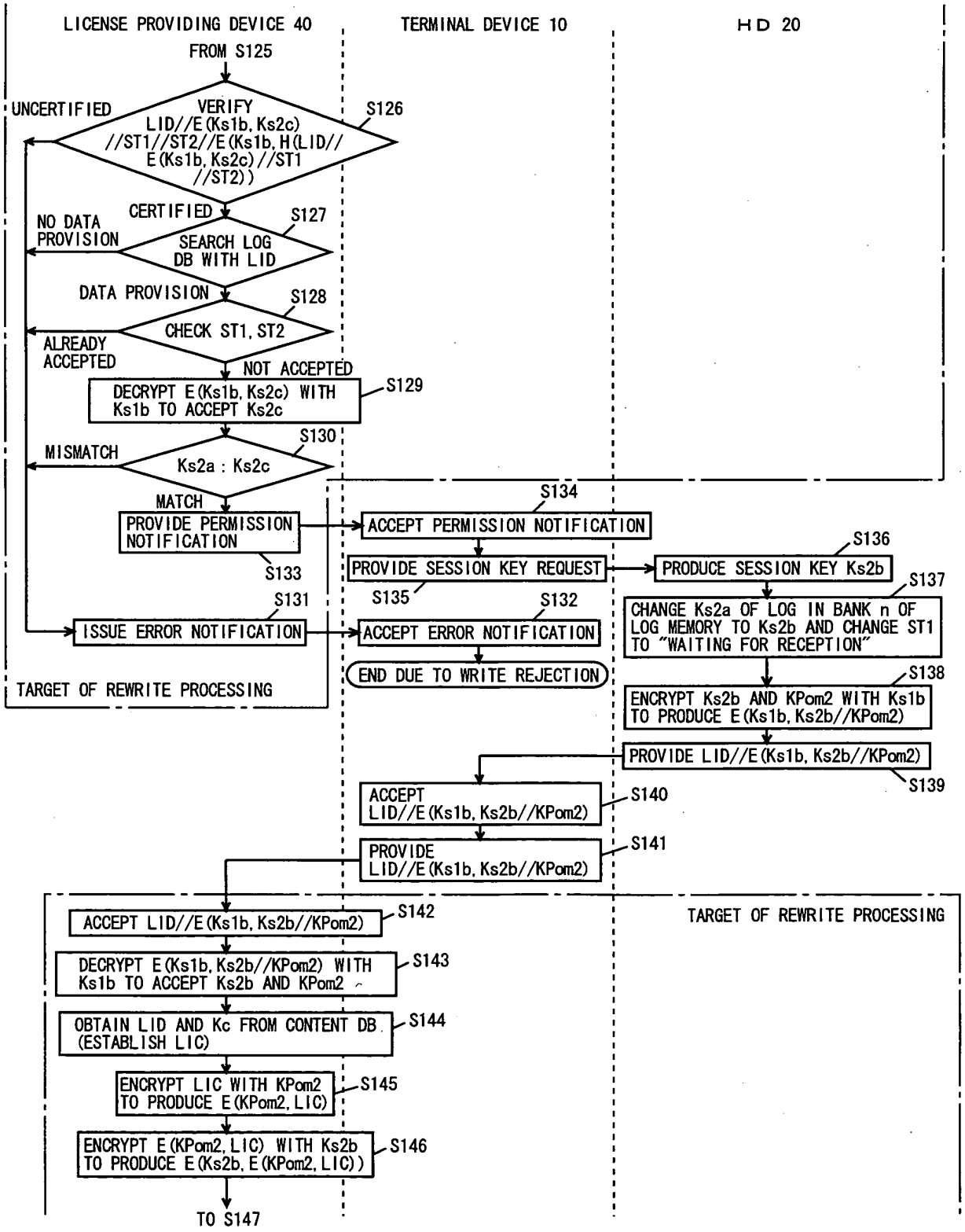


FIG. 15

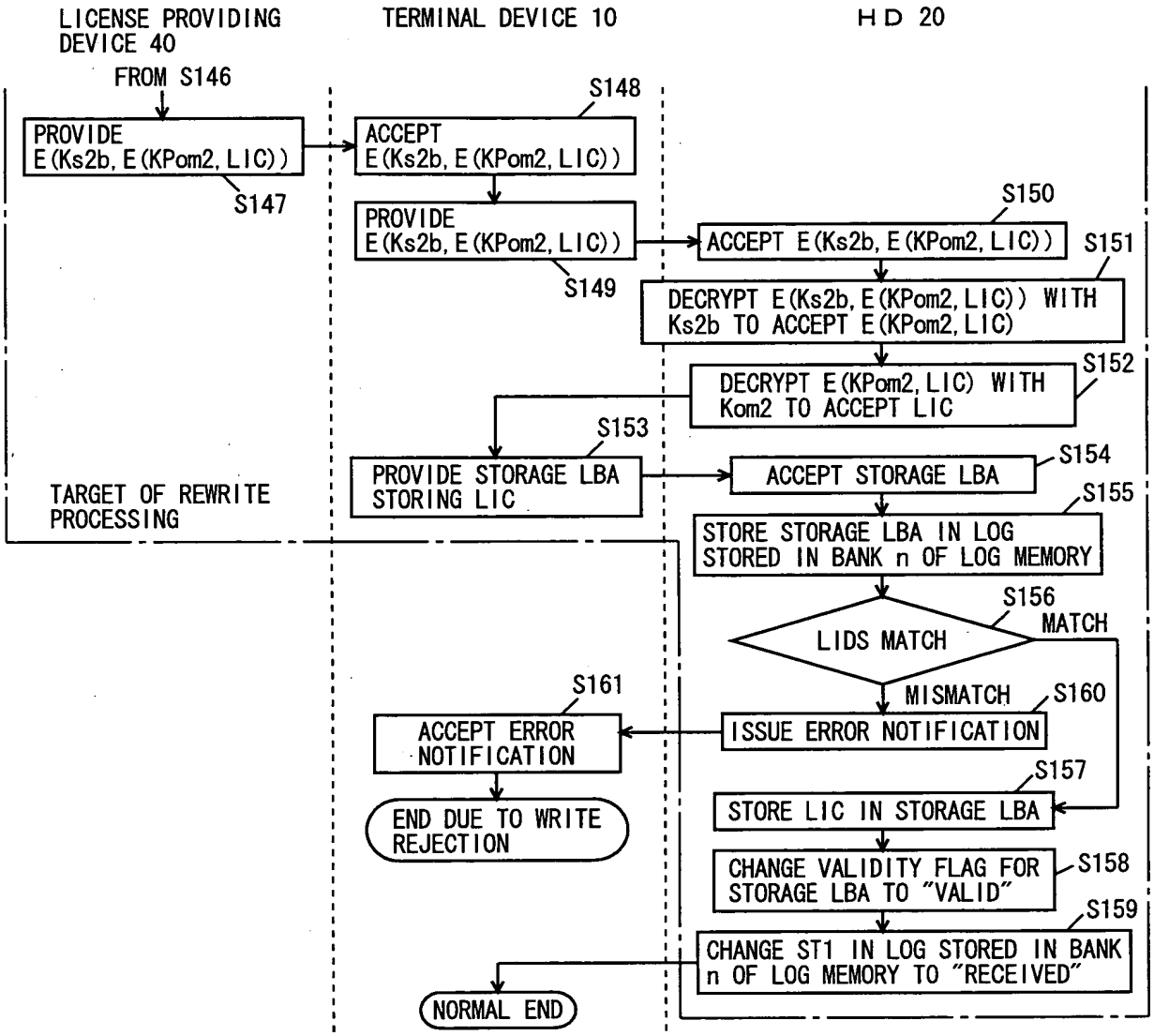
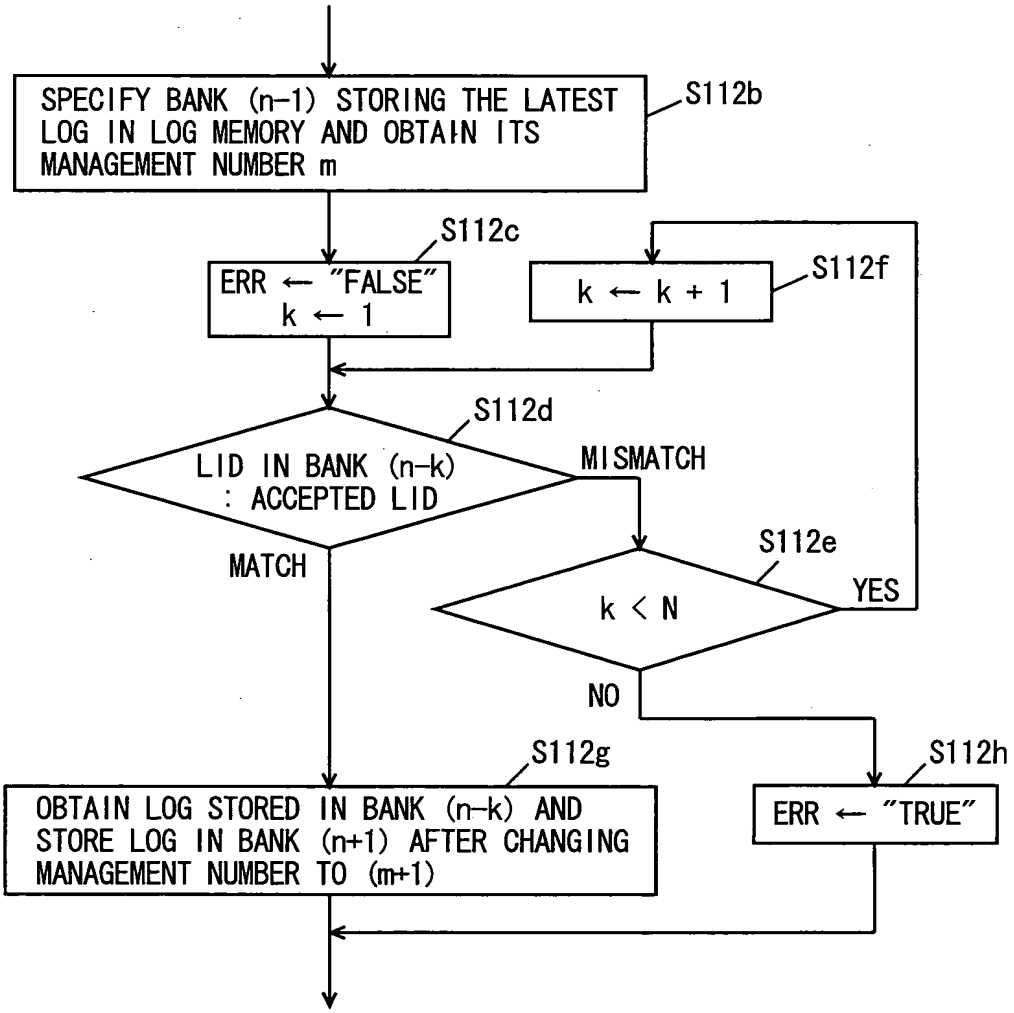


FIG. 16



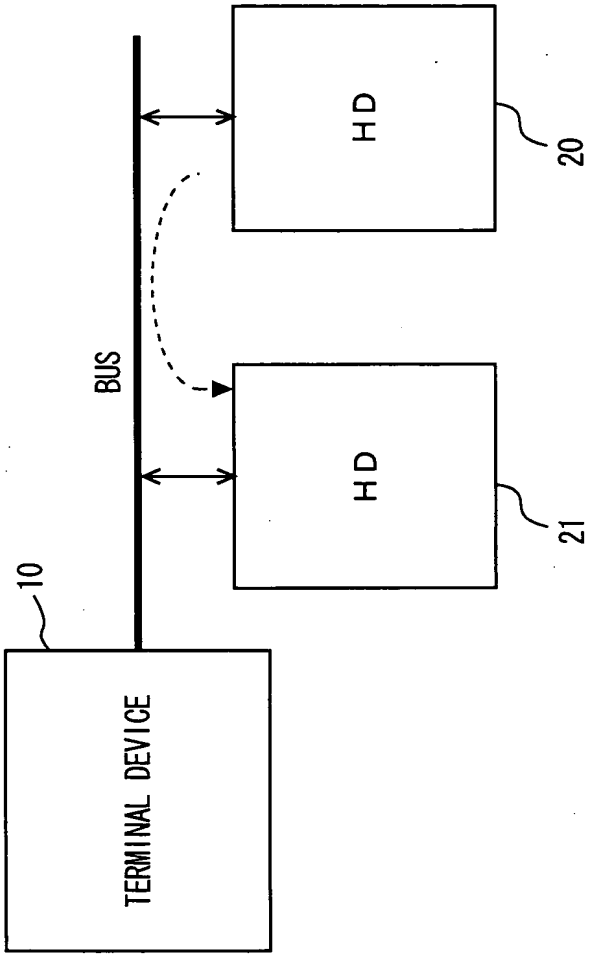


FIG. 17

FIG. 18

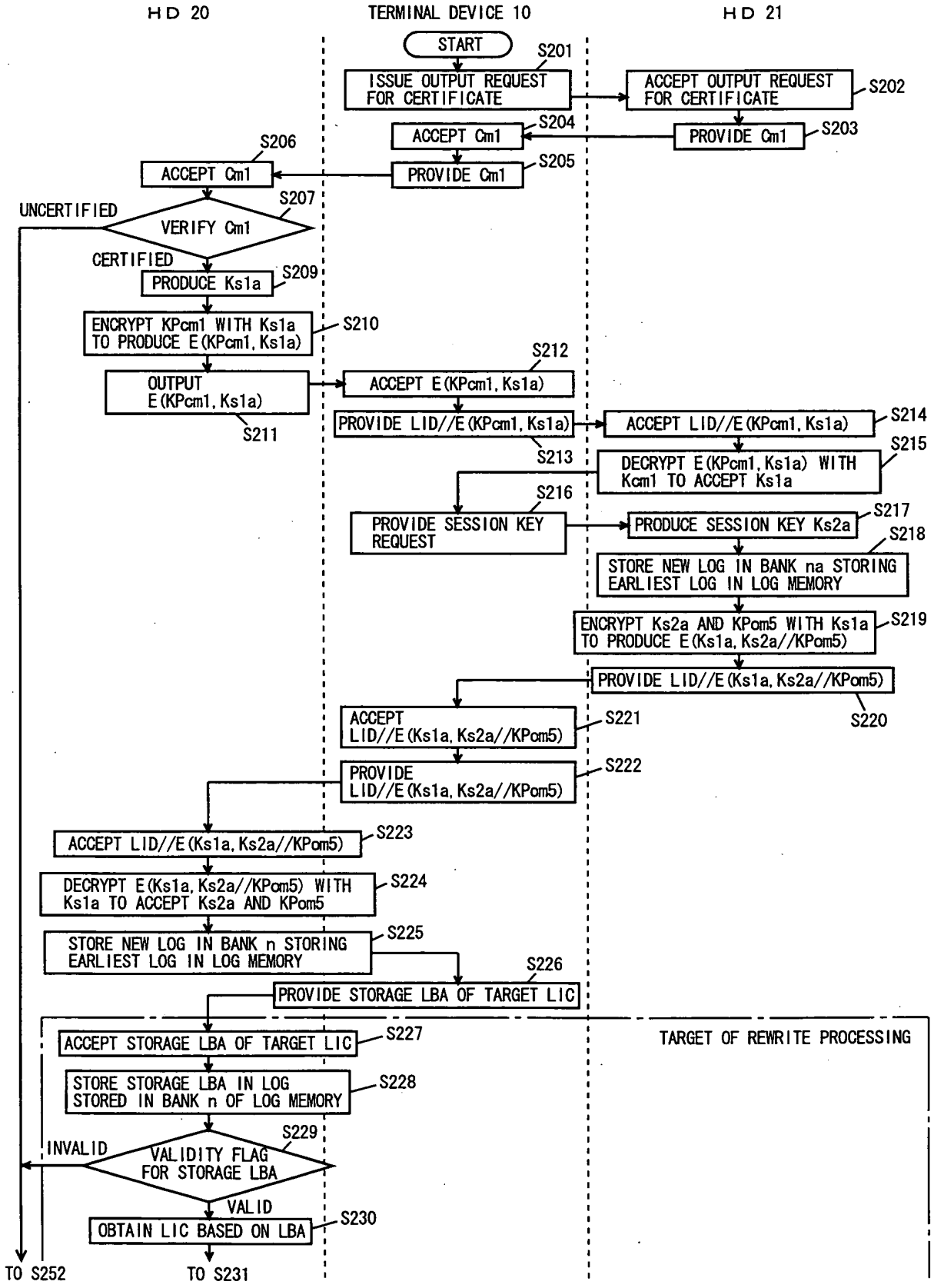


FIG. 19

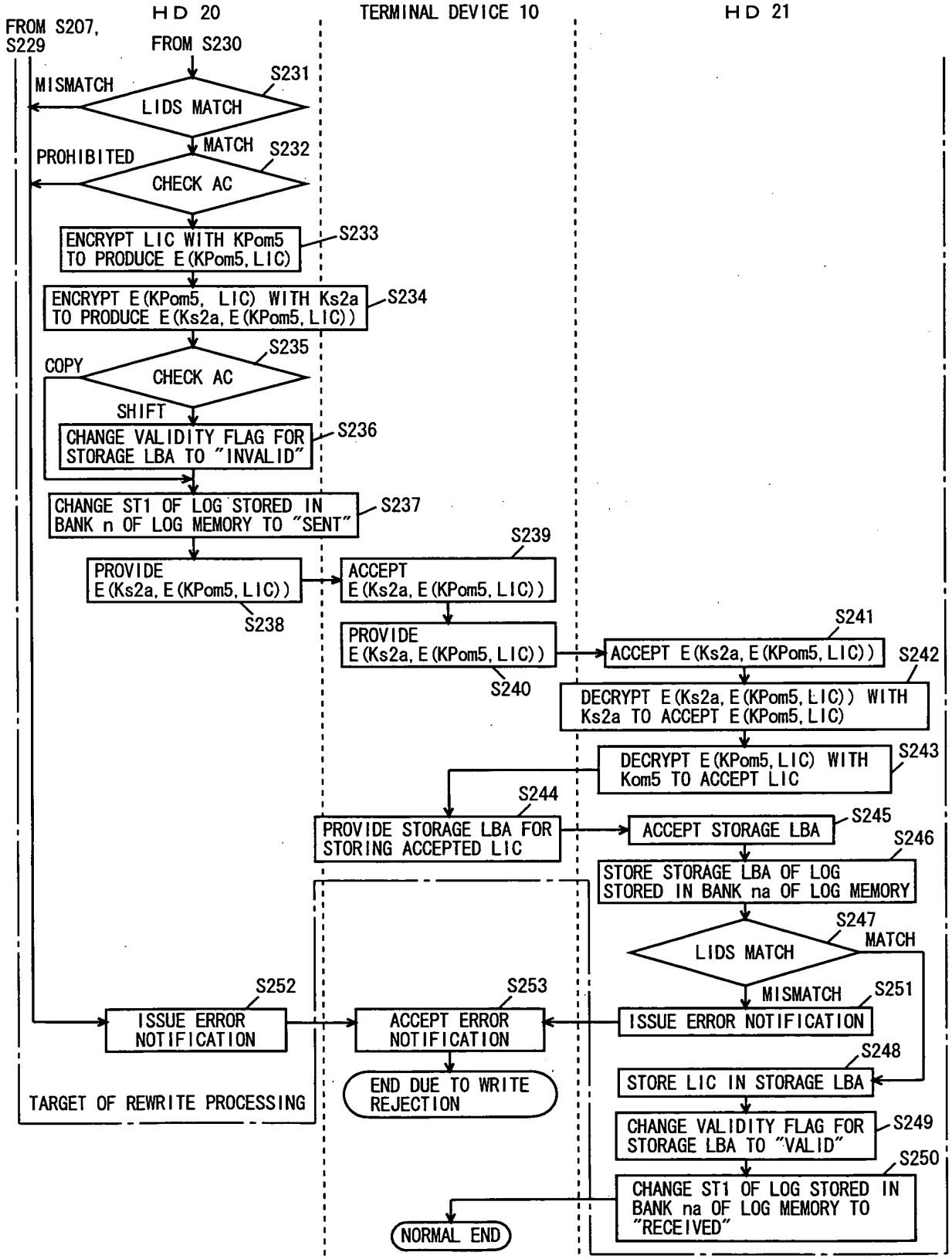


FIG. 20

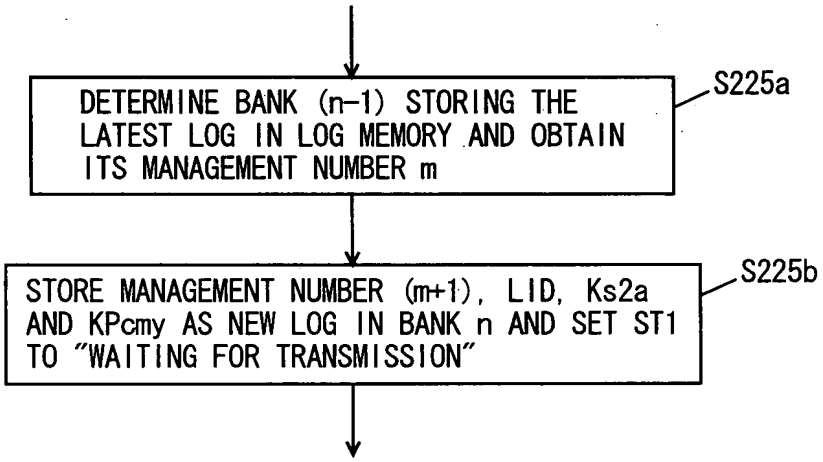


FIG. 21

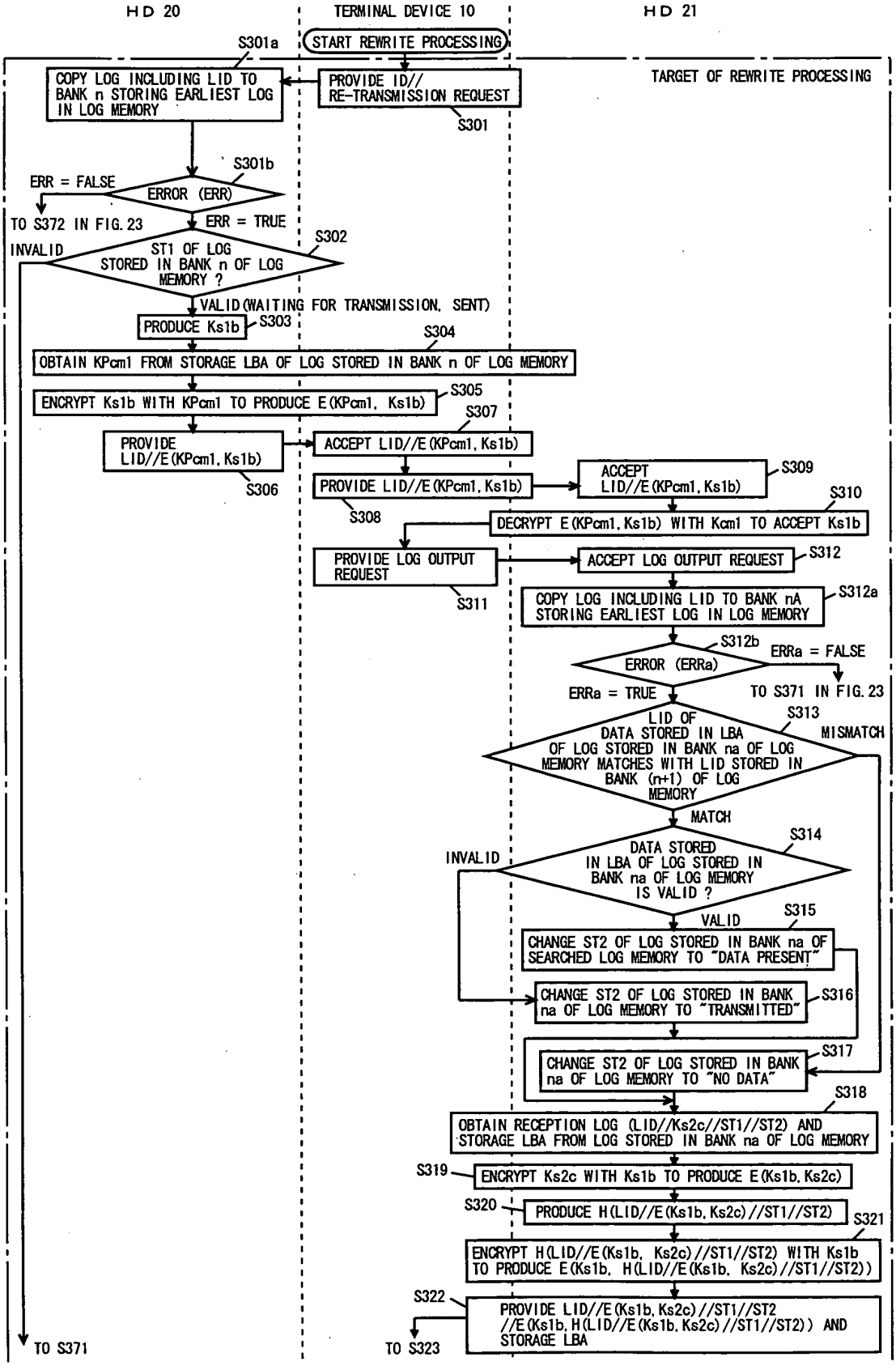


FIG. 22

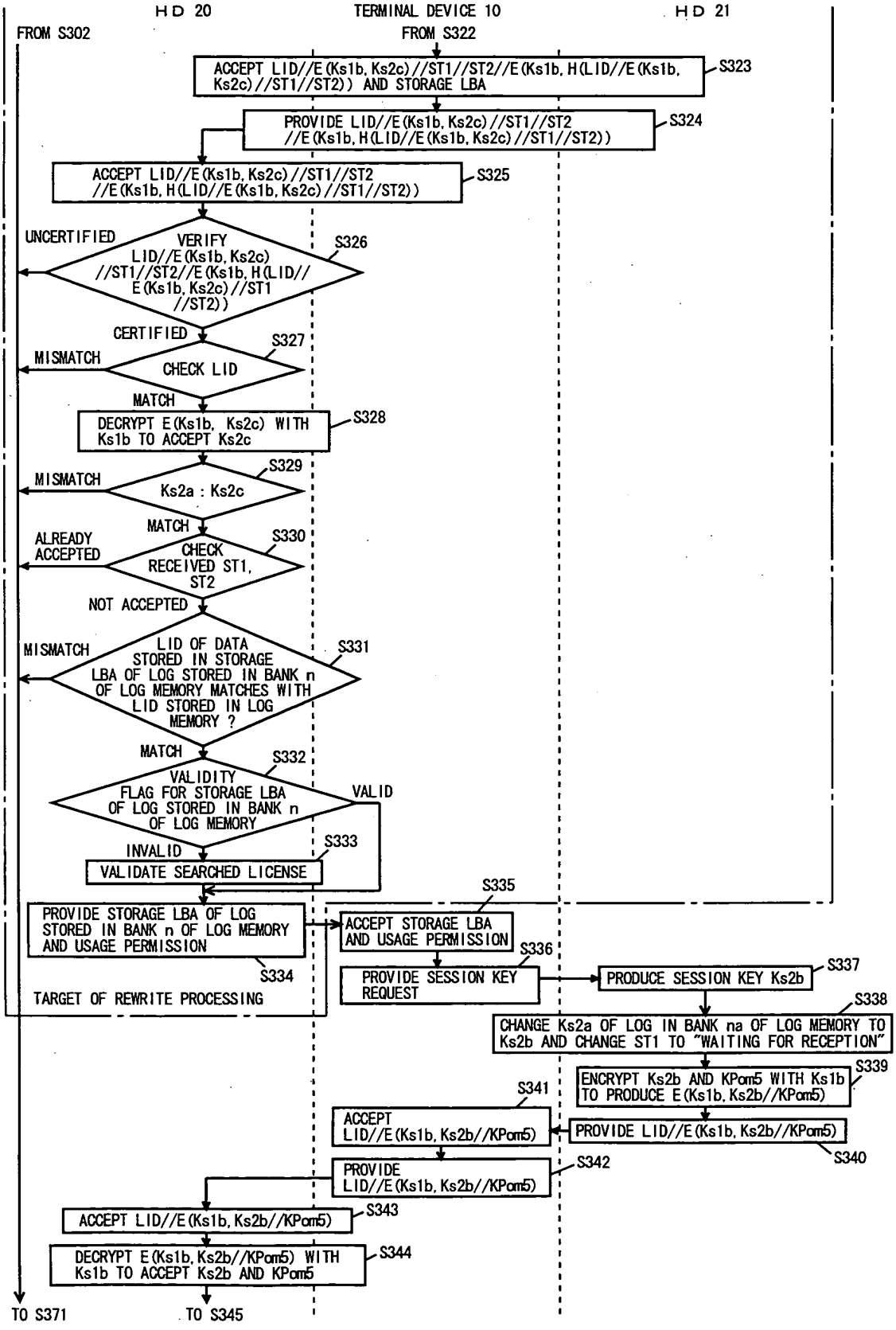

HD 20
TERMINAL DEVICE 10
HD 21
FROM S302
FROM S322
ACCEPT LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2)) AND STORAGE LBA
S323
PROVIDE LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))
S324
ACCEPT LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))
S325
UNCERTIFIED
VERIFY LID//E(Ks1b, Ks2c) //ST1//ST2//E(Ks1b, H(LID// E(Ks1b, Ks2c)//ST1 //ST2))
S326
CERTIFIED
MISMATCH
CHECK LID
S327
MATCH
DECRYPT E(Ks1b, Ks2c) WITH Ks1b TO ACCEPT Ks2c
S328
MISMATCH
Ks2a : Ks2c
S329
MATCH
ALREADY ACCEPTED
CHECK RECEIVED ST1, ST2
S330
NOT ACCEPTED
MISMATCH
LID OF DATA STORED IN STORAGE LBA OF LOG STORED IN BANK n OF LOG MEMORY MATCHES WITH LID STORED IN LOG MEMORY ?
S331
MATCH
VALIDITY FLAG FOR STORAGE LBA OF LOG STORED IN BANK n OF LOG MEMORY
S332
VALID
INVALID
VALIDATE SEARCHED LICENSE
S333
PROVIDE STORAGE LBA OF LOG STORED IN BANK n OF LOG MEMORY AND USAGE PERMISSION
S334
TARGET OF REWRITE PROCESSING
S335
ACCEPT STORAGE LBA AND USAGE PERMISSION
S336
PROVIDE SESSION KEY REQUEST
PRODUCE SESSION KEY Ks2b
S337
CHANGE Ks2a OF LOG IN BANK na OF LOG MEMORY TO Ks2b AND CHANGE ST1 TO "WAITING FOR RECEPTION"
S338
ENCRYPT Ks2b AND KPom5 WITH Ks1b TO PRODUCE E(Ks1b, Ks2b//KPom5)
S339
S341
ACCEPT LID//E(Ks1b, Ks2b//KPom5)
PROVIDE LID//E(Ks1b, Ks2b//KPom5)
S340
PROVIDE LID//E(Ks1b, Ks2b//KPom5)
S342
ACCEPT LID//E(Ks1b, Ks2b//KPom5)
S343
DECRYPT E(Ks1b, Ks2b//KPom5) WITH Ks1b TO ACCEPT Ks2b AND KPom5
S344
TO S371
TO S345

FIG. 23

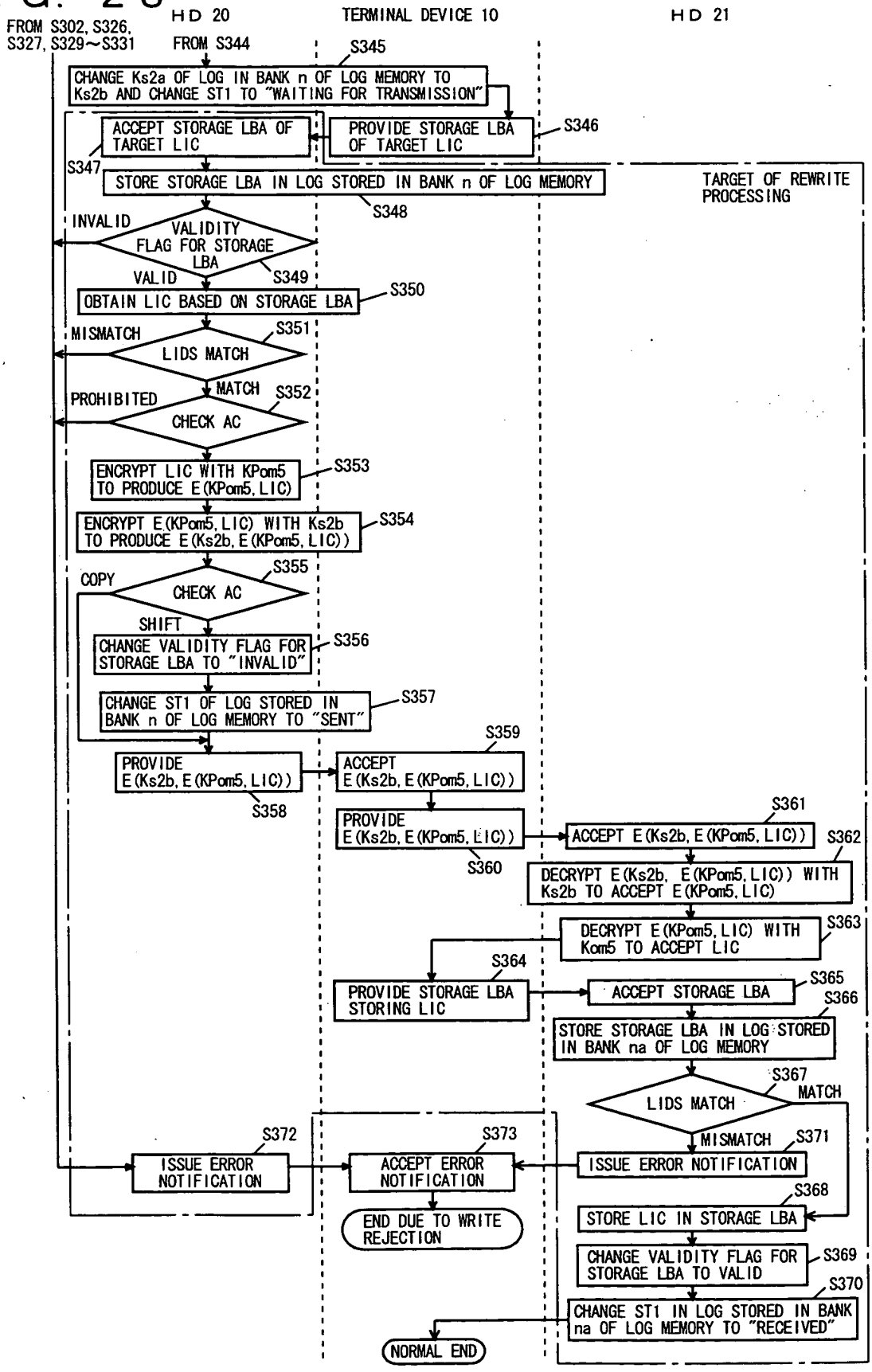


FIG. 24

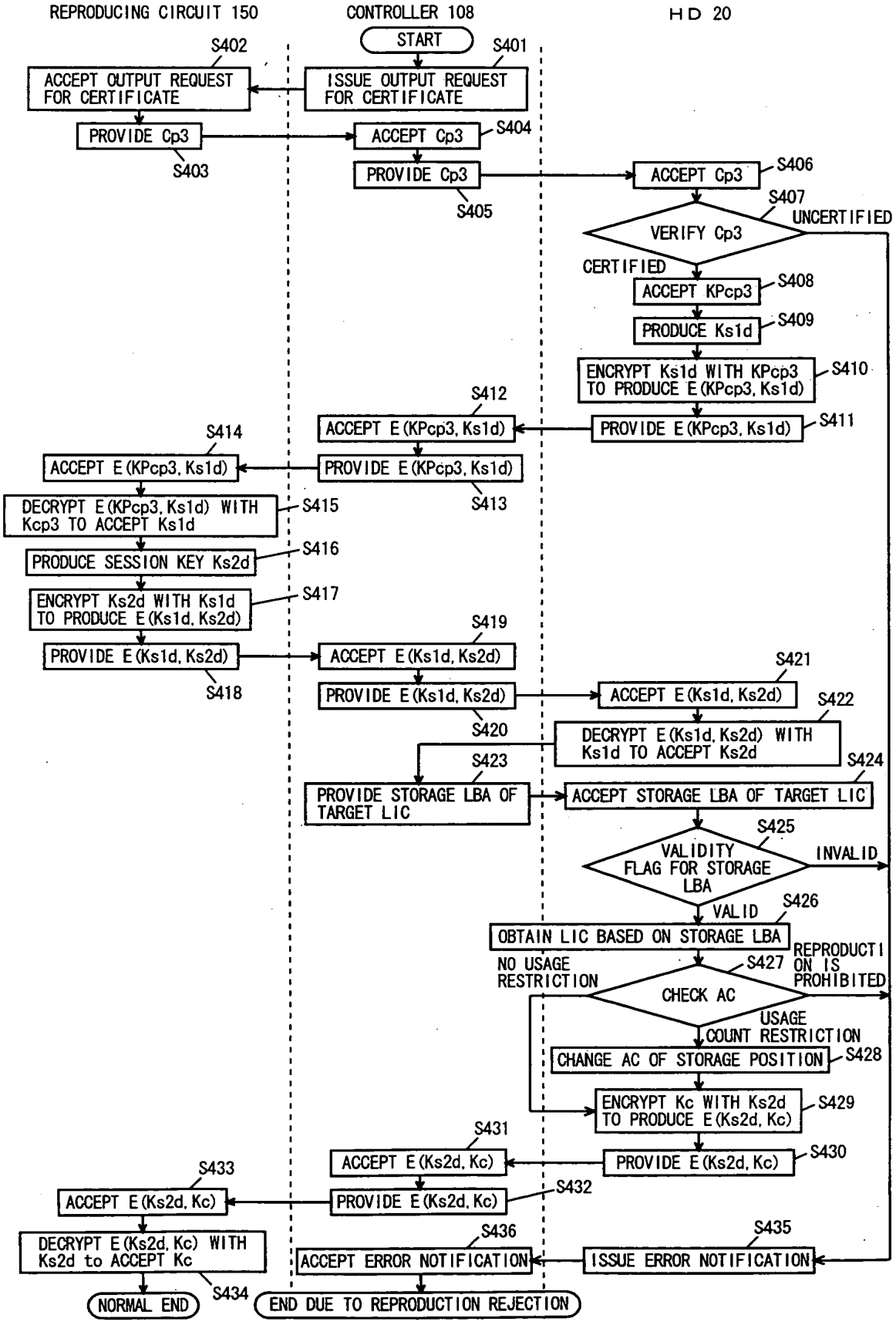


FIG. 25

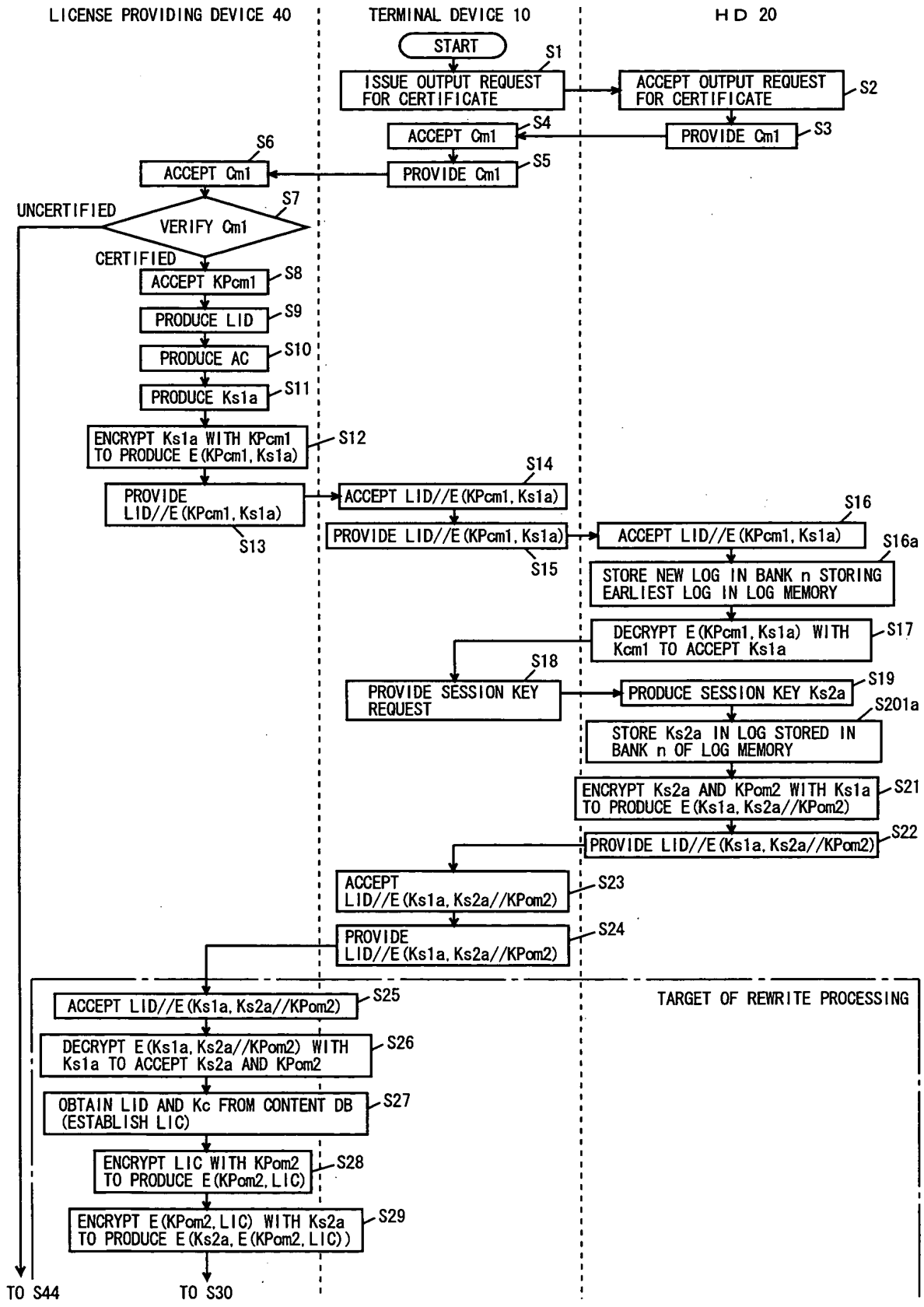


FIG. 26

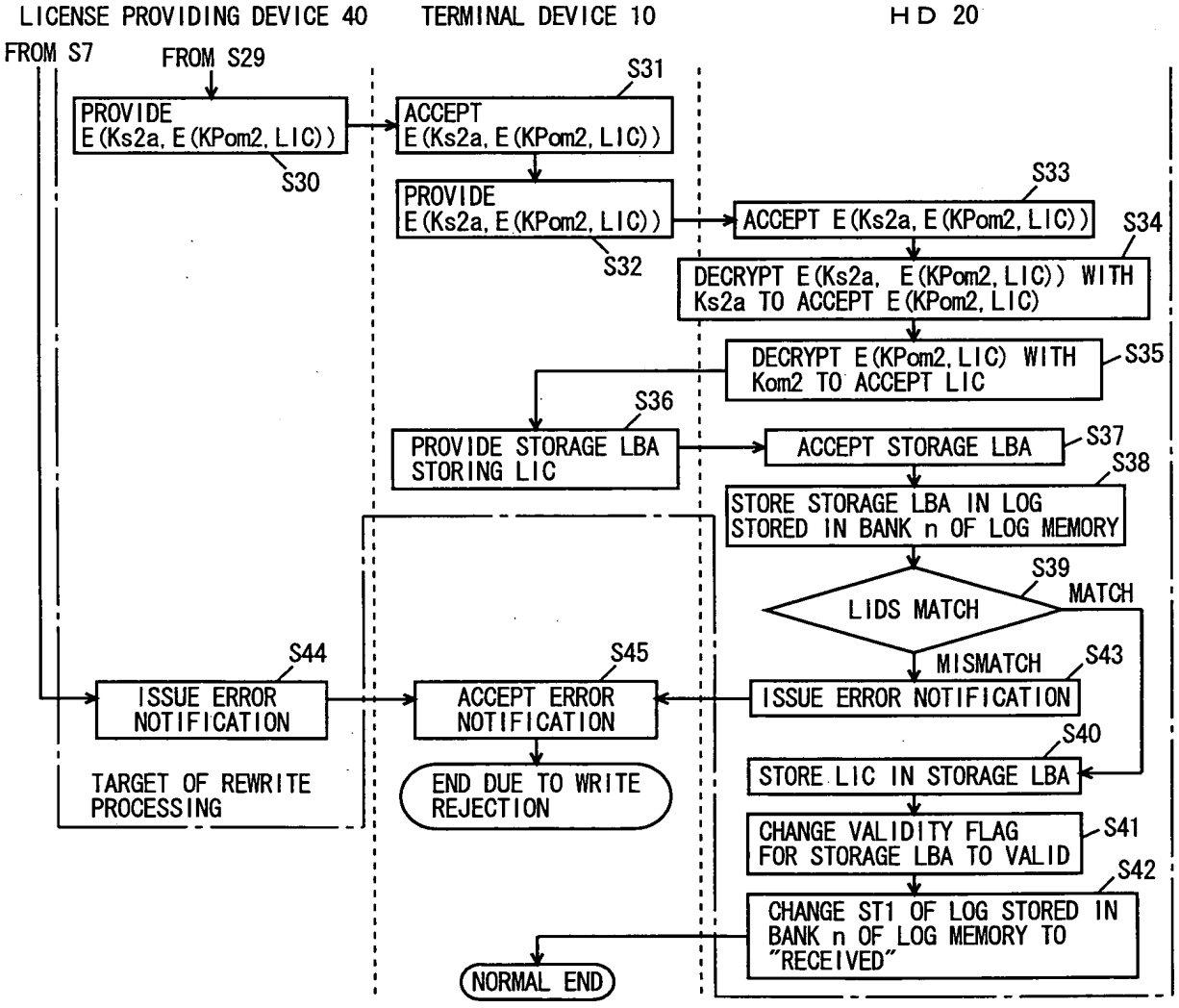


FIG. 27

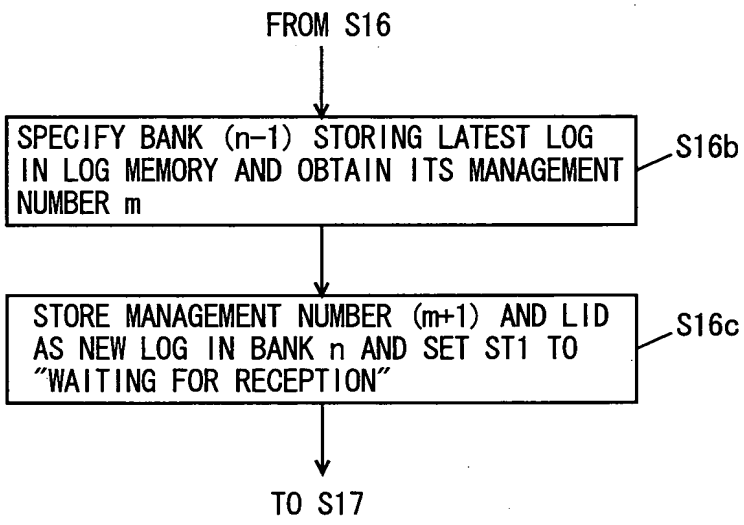


FIG. 28

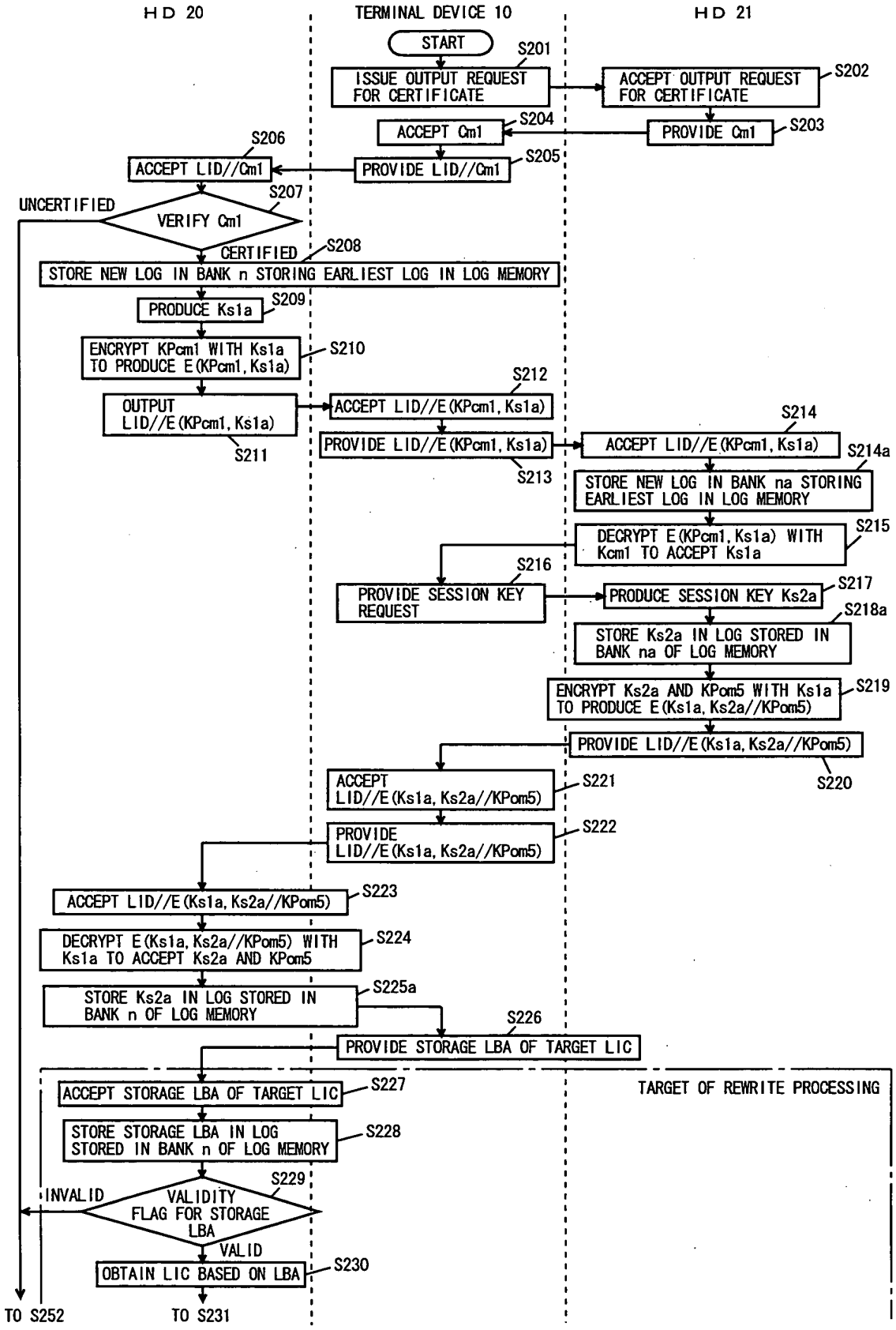


FIG. 29

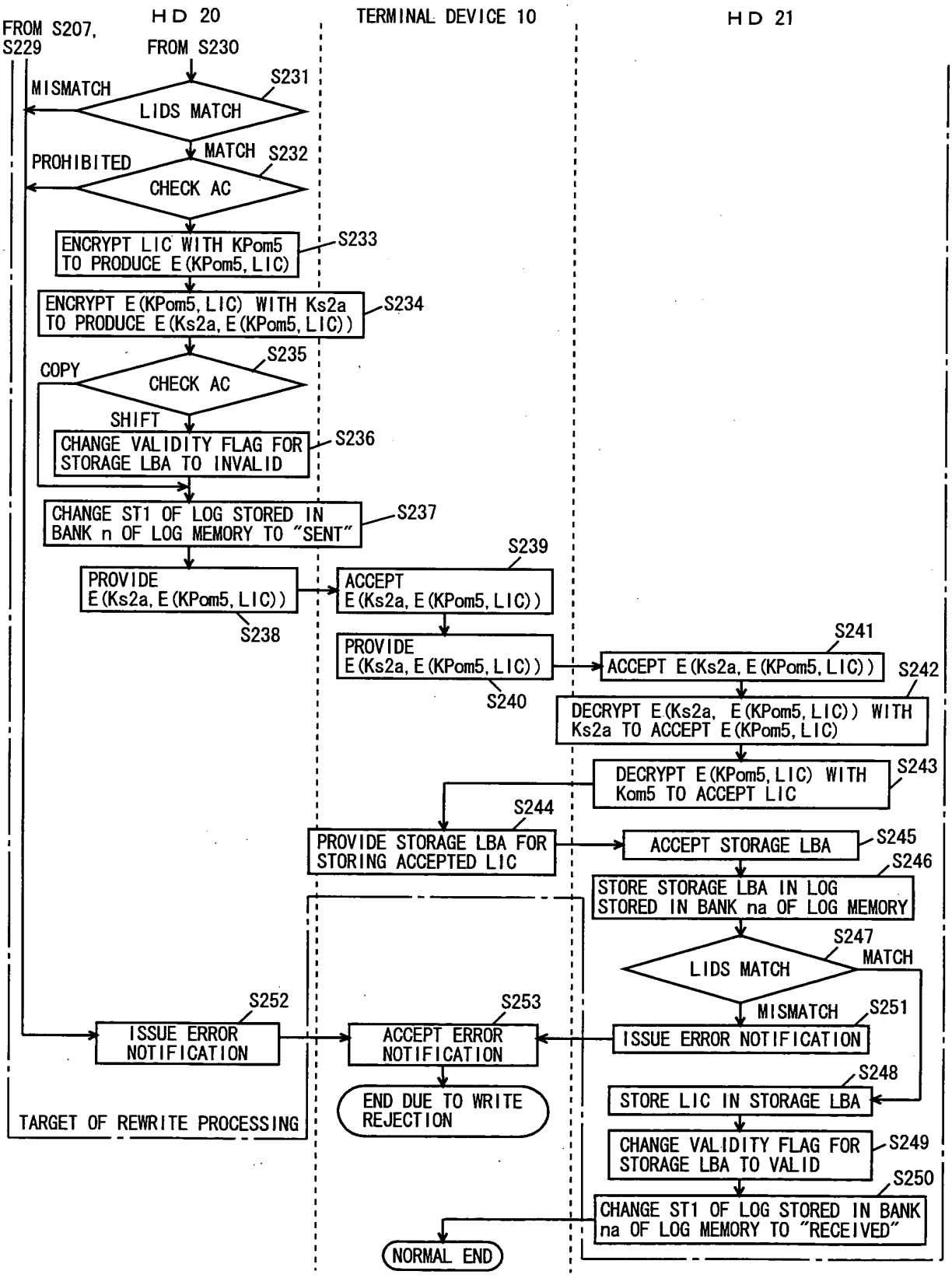


FIG. 30